70+ Vital Linux Commands Every Cybersecurity Analyst Should Master

No	Command	Description	Example
1	`pwd`	Prints the current working directory.	`pwd` displays the full path of the current directory.
2	`ls`	Lists directory contents.	`ls -l` lists files in long format, showing permissions, owner, size, and modification date. `ls -a` lists files including hidden files (those starting with a dot) `ls -la` list directory contents in a long format, including hidden files.
3	`cd`	Changes the current directory.	`cd /home/user` changes the directory to /home/user.
4	`touch`	Creates an empty file or updates the timestamp of an existing file.	`touch newfile.txt` creates an empty file named `newfile.txt`.

5	`echo`	Displays a line of text or a variable value.	`echo "Hello, World!"`
			prints Hello, World! to the terminal.
			`echo "Hello, World!" > filename.txt`
			creates a new text file named "filename.txt" (or overwrites it if it already exists) and writes the phrase "Hello, World!" into it.
			`echo "Hello, World!" >> filename.txt`
			appends the phrase "Hello, World!" to the end of the existing file named "filename.txt" (or creates the file if it doesn't exist).

6	`rm`	Removes files or directories.	`rm file.txt` deletes file.txt.
7	`cp`	Copies files or directories.	`cp file1.txt file2.txt` copies file1.txt to file2.txt. `cp file1.txt ./Desktop` copies the file named "file1.txt" from the current directory to the Desktop folder.
8	`mv`	used for moving and renaming files and directories.	`mv oldname.txt newname.txt` renames oldname.txt to newname.txt in the current directory. `mv file1.txt ./Desktop` moves the file named "file1.txt" from the current directory to the Desktop folder.
11	`cat`	Concatenates and displays file content.	`cat file.txt` displays the content of file.txt.
9	`nano`	Open the Nano text editor.	`nano file.txt` opens file.txt in the Nano editor.
10	`vim`	Open the Vim text editor.	`vim file.txt` opens file.txt in the Vim editor.
10	`shred`	Overwrites a file to hide its contents and optionally deletes it.	`shred -u file.txt` overwrites and deletes file.txt.
11	`mkdir`	Creates a new directory.	`mkdir newdir` creates a directory named newdir.
14	`rmdir`	Removes an empty directory.	`rmdir olddir` removes the empty directory olddir.
15	`ln`	Creates hard and symbolic links.	`ln -s target linkname` creates a symbolic link named `linkname` pointing to target.

16	`clear`	Clears the terminal screen.	`clear` clears the terminal display.
17	`whoami`	Displays the current logged-in user.	`whoami` shows the username of the current user.
18	`useradd`	Adds a new user.	`sudo useradd newuser` adds a new user named `newuser`.
19	`sudo`	Executes a command as another user, typically the superuser.	`sudo apt-get update` runs the `apt-get update` command with superuser privileges.
20	`adduser`	Adds a new user with a more interactive interface.	`sudo adduser newuser` interactively adds a new user named `newuser`.
21	`su`	Switch to another user account.	`su - user` switches to the `user` account.
22	`exit`	Exits the current shell or session.	`exit` logs out of the current session.
23	`passwd`	Changes a user's password.	`passwd` prompts to change the current user's password.
24	`apt`	Manages packages on Debian-based systems.	`sudo apt install package` installs the specified package. `sudo apt remove package` removes the specified package. `apt update` update the package list `apt upgrade` upgrade installed packages to their latest versions `apt dist-upgrade` perform a comprehensive system upgrade

1	`ssh`	Connects to a remote machine via SSH.	`ssh user@hostname` connects to the remote machine `hostname` as `user`.
25	`finger`	Displays information about system users.	`finger user` shows details about `user`.
26	`man`	Displays the manual page for a command.	`man ls` shows the manual for the `ls` command.
27	`whatis`	Displays a brief description of a command.	`whatis ls` provides a short description of the `ls` command.
28	`curl`	Transfers data from or to a server.	`curl -O http://example.com/file.txt` downloads `file.txt` from the specified URL.
29	`zip`	Compresses files into a zip archive.	`zip archive.zip file1 file2` compresses file1 and file2 into archive.zip.
30	`unzip`	Extracts files from a zip archive.	`unzip archive.zip` extracts files from archive.zip.
31	`less`	Views file content one screen at a time.	`less file.txt` displays file.txt content one screen at a time.
32	`head`	Displays the first part of a file.	`head -n 10 file.txt` shows the first 10 lines of `file.txt`.
33	`tail`	Displays the last part of a file.	`tail -n 10 file.txt` shows the last 10 lines of `file.txt`.
34	`cmp`	Compare two files byte by byte.	`cmp file1 file2` compares `file1` and `file2`.

35	`diff`	Compares files line by line.	`diff file1 file2` shows the differences between `file1` and `file2`.
36	`sort`	Sorts lines of text files.	`sort file.txt` sorts the lines in `file.txt`.
37	`find`	Searches for files in a directory hierarchy.	`find /home -name "*.txt"` finds all `.txt` files in the `/home` directory.
38	`chmod`	Changes file permissions.	`chmod 755 script.sh` sets the permissions of `script.sh` to `rwxr-xr-x`.
39	`chown`	Changes file owner and group.	`chown user:group file.txt` changes the owner and group of `file.txt` to `user` and `group`.
40	`ifconfig`	Display network interface information. Configures network interfaces.	`ifconfig eth0` displays the configuration of the `eth0` interface.
41	`ip address`	Displays IP addresses and interfaces.	`ip address show` shows all IP addresses and network interfaces.
42	`grep`	Searches for patterns in files.	`grep "pattern" file.txt` searches for "pattern" in `file.txt`.
43	`awk`	A programming language for pattern scanning and processing.	`awk '{print $1}' file.txt` prints the first field of each line in `file.txt`.
44	`resolvectl status`	Shows the current DNS settings.	`resolvectl status` displays the DNS configuration and status.
45	`ping`	Sends ICMP ECHO_REQUEST packets to network hosts.	`ping google.com` sends ping requests to `google.com`.

46	`netstat`	Displays network connections, routing tables, and interface statistics.	`netstat -tuln` shows listening ports and their status.
47	`ss`	Displays socket statistics.	`ss -tuln` shows listening sockets. `ss -l4p` displays all listening IPv4 sockets along with the associated processes
48	`iptables`	Configures packet filtering rules.	`sudo iptables -L` lists all current iptables rules.
49	`ufw`	Manages firewall with Uncomplicated Firewall.	`sudo ufw enable` enables the firewall.
50	`uname`	Prints system information.	`uname -a` displays all system information.
51	`neofetch`	Displays system information with an aesthetic layout.	`neofetch` shows system information in a visually appealing format.
52	`cal`	Displays a calendar.	`cal` shows the current month's calendar.
53	`free`	Displays memory usage.	`free -h` shows memory usage in a human-readable format.
54	`df`	Displays disk space usage of file systems.	`df -h` shows disk space usage in a human-readable format.
55	`ps`	Displays information about active processes.	`ps aux` shows detailed information about all running processes.
56	`top`	Displays real-time system resource usage.	`top` shows real-time processes and system resource usage.

57	`htop`	An interactive process viewer.	`htop` provides an interactive view of system processes.
58	`kill`	Terminates a process by PID.	`kill 1234` terminates the process with PID 1234.
59	`pkill`	Terminates processes by name.	`pkill firefox` terminates all processes named `firefox`.
60	`systemctl`	Manages systemd services.	`systemctl status nginx` shows the status of the `nginx` service.
61	`history`	Displays the command history.	`history` shows the list of previously executed commands.
62	`reboot`	Reboots the system.	`sudo reboot` restarts the system.
63	`shutdown`	Shuts down or reboots the system.	`sudo shutdown -h now` shuts down the system immediately.
64	`traceroute`	Traces the route packets take to a network host.	`traceroute google.com` shows the route to `google.com`.
65	`dig`	Queries DNS servers.	`dig example.com` retrieves DNS information for `example.com`.
66	`host`	Performs DNS lookups.	`host example.com` shows the IP address of `example.com`.
67	`arp`	Displays and modifies the ARP table.	`arp -a` shows the current ARP table.

68	`iwconfig`	Configures wireless network interfaces.	`iwconfig wlan0` shows the configuration of the `wlan0` wireless interface.
69	`hostname`	Displays or sets the system's hostname.	`hostname` shows the current hostname.
70	`whois`	Queries the WHOIS database for domain information.	`whois example.com` retrieves WHOIS information for example.com.